The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/18/2020

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox and Thunderbird Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) and Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Mozilla Thunderbird is an email client. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 83
- Mozilla Firefox ESR versions prior to 78.5
- Mozilla Thunderbird versions prior to 78.5

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) and Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A parsing and event loading mismatch in Firefox's SVG code could have allowed load events to fire, even after sanitization. An attacker already capable of exploiting an XSS vulnerability in privileged internal pages could have used this attack to bypass our built-in sanitizer. (CVE-2020-26951)
- When drawing a transparent image on top of an unknown cross-origin image, the Skia library drawImage function took a variable amount of time depending on the content of the underlying image. This resulted in potential cross-origin information exposure of image content through timing side-channel attacks. (CVE-2020-16012)
- It was possible to cause the browser to enter fullscreen mode without displaying the security UI; thus making it possible to attempt a phishing attack or otherwise confuse the user. (CVE-2020-26953)
- In some cases, removing HTML elements during sanitization would keep existing SVG event handlers and therefore lead to XSS. (CVE-2020-26956)
- Firefox did not block execution of scripts with incorrect MIME types when the response was intercepted and cached through a ServiceWorker. This could lead to a cross-site script inclusion vulnerability, or a Content Security Policy bypass. (CVE-2020-26958)
- During browser shutdown, reference decrementing could have occured on a previously freed object, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. (CVE-2020-26960)
- In Freetype, if PNG images were embedded into fonts, the Load_SBit_Png function contained an integer overflow that led to a heap buffer overflow, memory corruption, and an exploitable crash. (CVE-2020-15999)
- When DNS over HTTPS is in use, it intentionally filters RFC1918 and related IP ranges from the responses as these do not make sense coming from a DoH resolver. However when an IPv4 address was mapped through IPv6, these addresses were erroneously let through, leading to a potential DNS Rebinding attack. (CVE-2020-26961)
- Mozilla developers Steve Fink, Jason Kratzer, Randell Jesup, Christian Holler, and Byron Campen reported memory safety bugs present in Firefox 82 and Firefox ESR 78.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2020-26968)
- Incorrect bookkeeping of functions inlined during JIT compilation could have led to memory corruption and a potentially exploitable crash when handling out-of-memory errors. (CVE-2020-26952)
- During browser shutdown, reference decrementing could have occured on a previously freed object, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. (CVE-2020-26959)
- Cross-origin iframes that contained a login form could have been recognized by the login autofill service, and populated. This could have been used in clickjacking attacks, as well as be read across partitions in dynamic first party isolation. (CVE-2020-26962)
- Repeated calls to the history and location interfaces could have been used to hang the browser. This was addressed by introducing rate-limiting to these API calls. (CVE-2020-26963)
- If the Remote Debugging via USB feature was enabled in Firefox for Android on an Android version prior to Android 6.0, untrusted apps could have connected to the feature

and operated with the privileges of the browser to read and interact with web content. The feature was implemented as a unix domain socket, protected by the Android SELinux policy; however, SELinux was not enforced for versions prior to 6.0. This was fixed by removing the Remote Debugging via USB feature from affected devices. (CVE-2020-26964)

- Some websites have a feature "Show Password" where clicking a button will change a password field into a textbook field, revealing the typed password. If, when using a software keyboard that remembers user input, a user typed their password and used that feature, the type of the password field was changed, resulting in a keyboard layout change and the possibility for the software keyboard to remember the typed password. (CVE-2020-26965)
- Searching for a single word from the address bar caused an mDNS request to be sent on the local network searching for a hostname consisting of that string; resulting in an information leak. Note: This issue only affected Windows operating systems. Other operating systems are unaffected. (CVE-2020-26966)
- When listening for page changes with a Mutation Observer, a malicious web page could confuse Firefox Screenshots into interacting with elements other than those that it injected into the page. This would lead to internal errors and unexpected behavior in the Screenshots code. (CVE-2020-26967)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Mozilla:

https://www.mozilla.org/en-US/security/advisories/mfsa2020-50/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-52/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15999
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26956

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26968